2018-03

Cyber War or Monkey Business? a Book Review by James J. Wirtz of Cyber War versus Cyber Realities by Brandon Valeriano and Ryan C. Maness

Wirtz, James J.

James J. Wirtz (2018) Cyber War or Monkey Business?, International Journal of Intelligence and CounterIntelligence, 31:2, 415-419, DOI: 10.1080/08850607.2018.1418586
http://hdl.handle.net/10945/59140

Cyber War or Monkey Business?

JAMES J. WIRTZ

Brandon Valeriano and Ryan C. Maness: *Cyber War versus Cyber Realities*
Oxford University Press, New York, 2015, 266 p., $29.95.

Between 4 and 7 September 2001, I attended the First Biennial Threat Reduction Conference that was sponsored by the Defense Threat Reduction Agency in Norfolk, Virginia. One of the panels featured a debate about the likelihood of mass casualty terrorism in the United States. One panelist asserted that such an event was unlikely—the Aum Shinrikyo sarin attack being a case in point. Although well-funded and left relatively unmolested by the authorities, cultists managed to kill only 13 people when they released a nerve agent in the Tokyo subway. Thus, inflicting mass casualties, even with sarin, was not easily accomplished. The threat of mass casualty terrorism was being exaggerated by scholars and pundits alike, the panelist asserted, urging the conferees to instead focus on plausible threats. The other panelist agreed that Aum Shinrikyo was inept but offered the obvious counterpoint: just because something has not occurred in the past does not guarantee that it will not occur in the future.

The next morning, I contemplated this wonderfully "academic" debate on a pleasant United Airlines flight from Dulles to San Francisco. Soon afterwards it occurred to me that when it comes to picking an itinerary

James J. Wirtz is Dean of the School of International Graduate Studies and former Chairman of the Department of National Security Affairs at the United States Naval Postgraduate School, Monterey, California. A former Chairman and Program Chairman of the Intelligence Studies Section of the International Studies Association (ISA), he has also been President of the International Security and Arms Control Section of the American Political Science Association. A graduate of the University of Delaware, with a Ph.D. from Columbia University, New York City, he is the author and co-author of several books on intelligence and arms control. In March 2016, he was named a Distinguished Senior Scholar by the ISA's Intelligence Studies Section at its annual meeting in Atlanta, Georgia.

or making observations about the future, timing is everything.

DOUBTING THE THREAT HYPE

Brandon Valeriano and Ryan Maness acknowledge the "timing" problem inherent in their well-reasoned and empirically based assessment of state cyber conflicts that occurred between 2001 and 2011. Nevertheless, in their view, cyber war is mostly hype, created by over-imaginative academics and a cyber security industry ready to profit from cyber anxieties. By contrast, their analysis reveals that, at least in the period considered, cyber conflict was limited in both scope and severity, and was largely characterized by espionage or hooliganism (defacement of government websites) that generally produced no lasting impact. They note that in the vast majority of cases the incompetence of the victim or the aid of a witting or unwitting accomplice had facilitated penetration of some system. Here the 2015 hack of the U.S. Office of Personnel Management, which compromised the personal information of just about everyone who had ever applied for or possessed a U.S. security clearance, comes to mind. The Stuxnet attack against Iranian centrifuges, an outlier in their database, is used to illustrate their fundamental point: that the use of cyber warfare to inflict real damage is a rare and extraordinarily difficult endeavor that is probably within the technical reach of only a few states.

Valeriano and Maness also back up their empirical observations with some theoretical musings about why the reality of cyber warfare is out of step with the cyber hype surrounding the issue. Zero-day exploits (using heretofore unknown system vulnerabilities) are fleeting in their efficacy; once revealed, they are quickly rectified. Because they begin to lose their effectiveness soon after they are employed, the tendency is to keep one's powder dry, so to speak. Moreover, aggressive viruses can either propagate uncontrollably across the Internet or be repackaged and returned to the sender with unpredictable consequences. Because predicting the impact of more aggressive cyber attacks is difficult, states tend to exhibit restraint in their use of cyber weapons. Put somewhat differently, weapons that are likely to produce collateral damage or even fratricide are not readily embraced by military professionals. Although the authors do not mention it, attitudes toward the use of cyber weapons seem to mirror the history of biological warfare. Unleashing contagion is highly unpredictable; weapons with unknowable effects have little military utility. They might produce their intended impact, but there is no telling how far disease might spread. Because the same can be said for cyber weapons, restraint characterizes the way states engage in cyber conflict.

Another theoretical insight offered by Valeriano and Maness is that cyber conflict is both profoundly political and strategic. Conflict is

centered on a set of enduring rivalries: India and Pakistan, China and Japan, Russia and member states of the former Soviet Union, the United States and China, and the United States and Iran. With the exception of Stuxnet, these incidents tend to be limited, matching the "short-of-war" levels of acrimony present in these relationships. These observations are important because some policymakers and scholars tend to focus on *what* might happen in cyberspace, not *why* it might happen. For instance, it is theoretically possible to temporarily bring down the power grid in the United States, or to disrupt the stock market, or to cripple the banking system, creating significant disruption or even loss of life. But in focusing on these scenarios observers fail to stipulate the strategic purpose or the political setting that would motivate the launch of a highly devastating cyber attack. Admittedly, for those on the front lines of cyber defense, it might appear that the world has descended into a feral state of nature as they monitor thousands of attempts daily to hack into protected networks. Nevertheless, Valeriano and Maness correctly note that no one has yet died in a cyber attack, a requirement needed to turn an incident into a "war." In a political and strategic sense, the world has not yet witnessed cyber war.

ALTERING THE SCENARIO

So, what could alter the relatively benign picture of cyber conflict portrayed in *Cyber War versus Cyber Realities?* Valeriano and Maness would suggest that the future will mirror the past because cyber attacks are difficult to calibrate, execute, and control and generally do little more than create another round of cyber hype. Restraint will continue to characterize the emergence of cyber conflict in international affairs. Nevertheless, two considerations embedded in their analysis might temper expectations that the past will resemble the future regarding cyber conflict.

First, they embrace a U.S.-centric view of cyber warfare. They tend to treat cyber as a precision-guided weapon that can produce asymmetric physical effects by targeting key nodes or systems. Stuxnet is the quintessential example of this sort of attack—some well-placed computer code managed to temporarily sabotage the Iranian reprocessing effort. Nevertheless, other national "styles" have emerged when it comes to cyber conflict, giving doubt that the American approach is the most effective way to employ cyber as a weapon. The Russians, for example, see cyber as a truly strategic weapon, one intended to shape the political landscape in a way that suits the Kremlin's interests. Moscow devotes an enormous amount of effort to shaping content on the World Wide Web to skew stories and opinion to correspond to its view of the world and facilitate Russian foreign policy. The apparent Russian hack of the Democratic National Committee during the 2016 U.S. presidential

campaign is a case in point. Even though the hack constituted a minimum severity attack according to the threat matrix developed by Valeriano and Maness, it constituted a strategic use of a cyber weapon that might have produced a profound political impact, shaping the international setting to Moscow's liking. Additionally, China's "Great Wall" approach to cyber conflict, whereby the regime tightly controls its own domestic cyber space while working relentlessly to ferret out the (sometimes mundane) secrets of others, often appears quirky if not downright misguided. Nevertheless, as I consider the dystopia reflected on my Facebook feed, which is filled with partisan propaganda, fake news, and all sorts of social, class, and political agitation, the Chinese way of managing the World Wide Web appears less misguided. Beijing's approach to cyber conflict is an appropriate response to the agitprop generated on social media by domestic opposition movements or foreign sources (e.g., the Russian approach to cyber war). Cyber warfare, when it takes the form of something other than a precision-strike, might be where future cyber conflict is heading. The severity scale used by Valeriano and Maness to judge the threat posed by cyber conflict might need recalibration.

Second, and more telling, is the observation that even though *Cyber War versus Cyber Realities* cites technical and operational limitations as the primary source of cyber restraint, another factor might be moderating behavior in cyber space. Specifically, relatively benign political relations, not technical constraints, might be limiting the severity of cyber attacks. In other words, Valeriano and Maness are quite correct to tie the occurrence of cyber attacks to enduring rivalries—states do not harass other states "just because they can." Nevertheless, if these rivalries heat up, could an increase in the severity and impact of cyber conflict be expected? The relatively benign cyber conflicts that occurred between 2001 and 2011 might have been the product of a peaceful period in these rivalries, not the product of technical and operational constraints that are likely to restrain cyber attacks even in a deteriorating situation. Although states have not gone "all in" when regarding cyber war, the reality is that the political motivations for the eruption of full-scale hostilities have not been present either. Moderate political relations could easily account for the relatively benign nature of cyber conflict during the period considered by Valeriano and Maness.

Cyber War versus Cyber Realities makes a real contribution to the literature on cyber conflict by suggesting that, so far at least, cyber does not constitute a "silver bullet" when it comes to conflict. It also demonstrates that predictions of a coming Cyber Pearl Harbor must be tied to realistic strategic and political settings in order to be credible. Vulnerabilities are known, attack methods can be identified, and the

strategic impact of a successful cyber attack can be estimated in advance. What remains to be determined is when officials might feel politically compelled to take a gamble by going all in on cyber. To suggest how to make that prediction is difficult, but it is something to think about on that next flight from Dulles to San Francisco.

Once More into Laos

J. RANSOM CLARK

Joshua Kurlantzick: *A Great Place to Have a War: America in Laos and the Birth of a Military CIA*
Simon & Schuster, New York, 2016, 323 p., $28.00.

Joshua Kurlantzick provides a reasonably accurate (though not complete) view of the U.S. involvement in Laos from 1961 to 1975. Given the substantial body of existing literature detailing and dissecting the U.S. effort in Laos, however, to ask whether yet another assessment is needed is not unkind. To put it another way, is there anything new in his *A Great Place to Have a War: America in Laos and the Birth of a Military CIA*? Although the basic answer to that question is "not really," Kurlantzick does offer two "hooks" in seeking to bring some originality to the discussion. First, he asserts that the war in Laos gave birth to today's "militarized" Central Intelligence Agency (CIA); and second, he weaves into his narrative the roles and personalities

J. Ransom Clark, J.D., served twenty-five years with the Central Intelligence Agency, including assignments in Asia, Europe, Latin America, the Middle East, and Washington, D.C. After retiring from the Senior Intelligence Service, Professor Clark taught and held administrative positions at Muskingum University, New Concord, Ohio. The author of American Covert Operations: A Guide to the Issues *(Santa Barbara, CA: Praeger, 2015), his extensive Website on intelligence*—The Literature of Intelligence: A Bibliography of Materials, with Essays, Reviews, and Comments—*is at http://intellit.muskingum.edu. He is a member of the Editorial Advisory Board of the* International Journal of Intelligence and CounterIntelligence.